Information theoretic representations of qubit channels

Tanner Crowder* and Keye Martin†

Center for High Assurance Computer Systems (Code 5540)
Naval Research Laboratory
Washington D.C. 20375

Abstract

A set of qubit channels has a *classical representation* when it is isomorphic to the convex closure of a group of classical channels. From [5], we know that up to isomorphism there are five such sets, each corresponding to either a subgroup of the alternating group on four letters, or a subgroup of the symmetric group on three letters. In this paper, we show that the classical representation of a qubit channel also carries its *information theoretic* data – in particular, both the Holevo capacity and the scope of a unital qubit channel can be completely calculated from a systematically determined classical channel.

1 Introduction

In [5], the sets of qubit channels with classical representations were completely characterized up to isomorphism: they are $\langle G \rangle$, where G is a subgroup of either $\mathbb{A}_4$, the alternating group on four letters, or S_3, the symmetric group on three letters. This permits one to reason about such qubit channels as though they were classical channels, at least as far as their algebraic structure is concerned. But what about their information theoretic properties? For instance, can we determine the Holevo capacity of a qubit channel solely from its classical representation? Or its scope? Surprisingly, in this paper, we shall see that the answer to questions along this line is yes.

The underlying reason for why is that the isomorphisms associated to the five groups are all defined by conjugation, so practically any property of a qubit channel is also shared by its classical representation, including eigenvalues and singular values. This raises the question of which types of qubit channels have a classical representation, and we shall prove that the following all do: projective measurements, teleportation with a pure entangled state, the symmetric and skew-symmetric channels. In particular, this implies that both the Holevo capacity and the scope of *any* unital qubit channel can be calculated from a systematically determined classical channel.

*crowder@chacs.nrl.navy.mil

†kmartin@itd.nrl.navy.mil

2 Classical representations

Let (m, n) denote the set of stochastic matrices with m rows and n columns, the classical channels with m inputs and n outputs. The set of qubit channels $\mathcal{Q}$ consists of all affine transformations of the unit ball in $\mathbb{R}^3$ which arise as the Bloch representations of the convex linear, completely positive, trace preserving maps on 2×2 density matrices. The convex closure of X is $\langle X \rangle$.

All subgroups of matrices are assumed to have the identity matrix I as the group identity and to be nontrivial.

Definition 2.1 Let G be a subgroup of (m, n). An *embedding* of $\langle G \rangle$ into $\mathcal{Q}$ is a function $\varphi : \langle G \rangle \to \mathcal{Q}$ such that for all $x, y \in \langle G \rangle$,

- $\varphi(I) = I$,
- $\varphi(xy) = \varphi(x)\varphi(y)$,
- $\varphi(px + (1-p)y) = p\varphi(x) + (1-p)\varphi(y)$ whenever $p \in [0, 1]$, and
- $\varphi(x) = \varphi(y) \Rightarrow x = y$.

That is, an *embedding* is an injective, convex-linear homomorphism. The set of qubit channels $\varphi(\langle G \rangle)$ is then said to have a *classical representation*.

From [5], let us first recall the collections of qubit channels that have a classical representation: there are five of them, each one being either a subgroup of $\mathbb{A}_4$ or a subgroup of S_3, where one must use the *unorthodox copy* of $S_3 \subseteq (5, 5)$ given by

$$S_3 = \left\{ \begin{array}{ccc} I, & \bar{a} = \begin{pmatrix} I & 0 \\ 0 & a \end{pmatrix}, & \bar{a}^2 = \begin{pmatrix} I & 0 \\ 0 & a^2 \end{pmatrix} \\ \\ \bar{b} = \begin{pmatrix} f & 0 \\ 0 & b \end{pmatrix}, & \bar{c} = \begin{pmatrix} f & 0 \\ 0 & c \end{pmatrix}, & \bar{d} = \begin{pmatrix} f & 0 \\ 0 & d \end{pmatrix} \end{array} \right\}$$

with $\{I, a, a^2, b, c, d\} \subseteq (3, 3)$ the natural copy of the symmetric group on three letters and

$$f = \text{flip} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in (2, 2).$$

Theorem 2.2 ([5]) *Let $\mathbb{A}_4 \subseteq (4, 4)$ denote the alternating group on four letters and $S_3 \subseteq (5, 5)$ denote the unorthodox copy of the symmetric group on three letters. Then*

(i) *For each subgroup G of $\mathbb{A}_4$, there is an embedding $\varphi : \langle G \rangle \to \mathcal{Q}$.*

(ii) *For each subgroup G of S_3, there is an embedding $\varphi : \langle G \rangle \to \mathcal{Q}$.*

(iii) *If $G \subseteq (m, n)$ is a group for which such an embedding exists, then G is either a subgroup of $\mathbb{A}_4$ or a subgroup of S_3. That is, G must be isomorphic to either $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2^2$, S_3 or $\mathbb{A}_4$.*

We will now see that such isomorphisms are much more than isomorphisms: they not only preserve algebraic structure, they also preserve information theoretic data.

3 An information theoretic representation

The function $\varphi : \langle A_4 \rangle \to \mathcal{Q}$ given by

$$\varphi(f) = \begin{pmatrix} e+x-y-z & -a-b+c+d & -a_2+b_2+c_2-d_2 \\ -a_2-b_2+c_2+d_2 & e-x+y-z & a-b+c-d \\ -a+b+c-d & a_2-b_2+c_2-d_2 & e-x-y+z \end{pmatrix}.$$

where $f \in \langle A_4 \rangle$ is written

$$f = \begin{pmatrix} e+c+c_2 & x+b+d_2 & y+d+a_2 & z+a+b_2 \\ x+d+b_2 & e+a+a_2 & z+c+d_2 & y+b+c_2 \\ y+a+d_2 & z+d+c_2 & e+b+b_2 & x+c+a_2 \\ z+b+a_2 & y+c+b_2 & x+a+c_2 & e+d+d_2 \end{pmatrix}.$$

is an embedding [5].

Theorem 3.1 *The embedding $\varphi : \langle A_4 \rangle \to \mathcal{Q}$ is conjugation by*

$$H = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

That is, if we conjugate the classical channel

$$f = \begin{pmatrix} e+c+c_2 & x+b+d_2 & y+d+a_2 & z+a+b_2 \\ x+d+b_2 & e+a+a_2 & z+c+d_2 & y+b+c_2 \\ y+a+d_2 & z+d+c_2 & e+b+b_2 & x+c+a_2 \\ z+b+a_2 & y+c+b_2 & x+a+c_2 & e+d+d_2 \end{pmatrix}$$

by the Hadamard matrix H we obtain

$$HfH^t = \begin{pmatrix} 1 & 0 \\ 0 & \varphi(f) \end{pmatrix}.$$

As a consequence, f and $\varphi(f)$ have the same singular values, and since the singular values of $\varphi(f)$ determine its Holevo capacity, this quantity can also be calculated from f. In a related way, the scope of $\varphi(f)$ is also determined by f. The function $\varphi : \langle S_3 \rangle \to \mathcal{Q}$ defined by

$$\varphi(f) = \begin{pmatrix} x_0-x_3 & x_1-x_5 & x_2-x_4 \\ x_2-x_5 & x_0-x_4 & x_1-x_3 \\ x_1-x_4 & x_2-x_3 & x_0-x_5 \end{pmatrix}.$$

where $f \in \langle S_3 \rangle$ is written

$$f = \begin{pmatrix} x_0+x_1+x_2 & x_3+x_4+x_5 & 0 & 0 & 0 \\ x_3+x_4+x_5 & x_0+x_1+x_2 & 0 & 0 & 0 \\ 0 & 0 & x_0+x_3 & x_1+x_5 & x_2+x_4 \\ 0 & 0 & x_2+x_5 & x_0+x_4 & x_1+x_3 \\ 0 & 0 & x_1+x_4 & x_2+x_3 & x_0+x_5 \end{pmatrix},$$

is an embedding [5]. Just as was the case with $\mathbb{A}_4$, it is not at all obvious that the information theoretic properties of $\varphi(f)$ can be determined from f, but once again, they can be:

Theorem 3.2 *The embedding $\varphi : \langle S_3 \rangle \to \mathcal{Q}$ is conjugation by*

$$T = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{6}} \\ 0 & \frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & 0 & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & -\frac{1}{\sqrt{3}} & 0 \end{pmatrix}.$$

That is, if we conjugate the classical channel

$$f = \begin{pmatrix} x_0+x_1+x_2 & x_3+x_4+x_5 & 0 & 0 & 0 \\ x_3+x_4+x_5 & x_0+x_1+x_2 & 0 & 0 & 0 \\ 0 & 0 & x_0+x_3 & x_1+x_5 & x_2+x_4 \\ 0 & 0 & x_2+x_5 & x_0+x_4 & x_1+x_3 \\ 0 & 0 & x_1+x_4 & x_2+x_3 & x_0+x_5 \end{pmatrix},$$

by T, we obtain

$$TfT^t = \begin{pmatrix} I_2 & 0 \\ 0 & \varphi(f) \end{pmatrix}.$$

4 Type

In an effort to better understand $\langle \mathbb{A}_4 \rangle$ and $\langle S_3 \rangle$ as forms of quantum structure, we now take a closer look at the kinds of channels they contain.

Definition 4.1 A qubit channel f is said to be of *type* G when it belongs to $\langle G \rangle$ for some finite subgroup $G \subseteq SO(3)$.

This definition does not depend on the particular representation of the group used: if F and G are finite isomorphic subgroups of $SO(3)$, then they are conjugate [1], and thus $\langle F \rangle \simeq \langle G \rangle$. In particular, such an isomorphism preserves both scope and Holevo capacity.

Theorem 4.2 *Let f be a unital qubit channel.*

- *If $f = f^2$ is idempotent, then f is of type $\mathbb{A}_4$.*
- *If $f = f^t$ is symmetric, then f is of type $\mathbb{A}_4$.*
- *If $f = -f^t$ is skew-symmetric, then f is of type $\mathbb{A}_4$.*

Any rotation $f \in SO(3)$ of order four has neither type $\mathbb{A}_4$ nor type S_3.

In order then, the following all have type $\mathbb{A}_4$: (i) projective measurements, (ii) the channels that determine Holevo capacity and scope, (iii) the nonzero skew symmetric channels, which are precisely those with scope $[0,0]$ but positive Holevo capacity. Notice that

$$f = \begin{pmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{pmatrix}$$

is a skew-symmetric qubit channel iff $a^2 + b^2 + c^2 \leq 1/4$. Thus, $\mathbb{A}_4$ contains a wide range of behavior, including the teleportation channels that arise when one uses a source of entanglement that is not necessarily maximal [7].

5 Closing

A major goal is to try and determine the physical significance of the five groups. For instance, we can think of $\langle \mathbb{Z}_2 \rangle$ as being a "bit flip" or a "phase flip," while $\langle \mathbb{Z}_2 \times \mathbb{Z}_2 \rangle$ can be thought of as the process of teleportation [7]. We know less about $\langle \mathbb{Z}_3 \rangle$ and $\langle \mathbb{A}_4 \rangle$ in general and almost nothing about $\langle S_3 \rangle$, except that it is the free affine monoid over the symmetric group on three letters.

References

[1] M. Artin. *Algebra*. Prentice Hall, New Jersey, 1991.

[2] T.M. Cover and J.A. Thomas. *Elements of information theory*. Wiley, 1991.

[3] H. S. M. Coxeter. *Introduction to Geometry*. John Wiley and Sons, Inc. (1961), New York.

[4] H. S. M. Coxeter and W. O. J. Moser. *Generators and Relations for Discrete Groups*. Springer-Verlag (1965), Germany.

[5] T. Crowder and K. Martin. *Classical representations of qubit channels.* Proceedings of Quantum Physics and Logic, Electronic Notes in Theoretical Computer Science, 2009, to appear.

[6] R.A. Horn and C.R. Johnson. *Matrix Analysis*. Cambridge University Press, New York, 1985.

[7] K. Martin, J. Feng and S. Krishnan. *A free object in quantum information theory*. Proceedings of MFPS 2010, Electronic Notes in Theoretical Computer Science, to appear.

[8] K. Martin. *The scope of a quantum channel.* Proceedings of the Clifford Lectures, American Math Society, to appear.

[9] M. Nielsen and I. Chuang, Quantum computation and quantum information. Cambridge University Press, 2000.

[10] D. Serre. *Matrices: Theory and applications.* Springer-Verlag, Graduate Texts in Mathematics, 2000.